(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－51575

(43)公開日　平成９年(1997)２月18日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｑ　7/38			Ｈ０４Ｂ　7/26	１０９Ｒ	

審査請求　未請求　請求項の数12　ＯＬ　（全 11 頁）

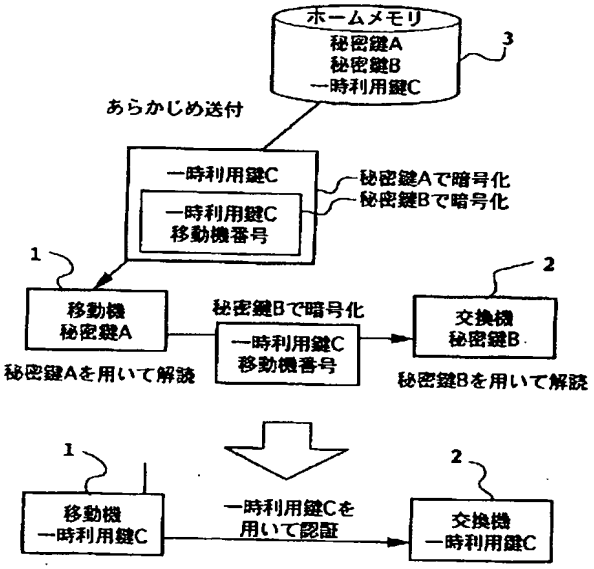
(21)出願番号　特願平7－199805

(22)出願日　平成７年(1995)８月４日

(71)出願人　392026693
エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番１号
(72)発明者　石田　創
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(72)発明者　大貫　雅史
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(72)発明者　中村　寛
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(74)代理人　弁理士　谷　義一　（外１名）

(54)【発明の名称】　移動通信における認証方法および移動通信システム

(57)【要約】
【課題】　認証によるホームメモリアクセス回数を減らす。
【解決手段】　ホームメモリ３が生成した一時利用鍵Ｃと暗号化された一時利用鍵Ｃとを移動機１が取得した後、移動機１から暗号化された一時利用鍵Ｃを交換機２に送信し、交換機２が復号化鍵を用いて暗号化された一時利用鍵Ｃを復号した後、移動機１と交換機２との間で共有した一時利用鍵Ｃにより認証を行う。



【特許請求の範囲】
【請求項１】　ホームメモリが生成した一時利用鍵と暗号化された一時利用鍵とを移動機が取得した後、前記移動機から前記暗号化された一時利用鍵を交換機に送信し、前記交換機が復号化鍵を用いて前記暗号化された一時利用鍵を復号した後、前記移動機と前記交換機との間で共有した前記一時利用鍵により認証を行うことを特徴とする移動通信における認証方法。
【請求項２】　請求項１において、前記移動機は、あらかじめ定めた限定された地域範囲毎に前記ホームメモリが新たに生成した一時利用鍵および暗号化された一時利用鍵を取得することを特徴とする移動通信における認証方法。
【請求項３】　請求項１において、前記交換機は、前記復号化鍵を時間の経過に従って変更することによって前記一時利用鍵の利用できる時間を制限することを特徴とする移動通信における認証方法。
【請求項４】　移動機に与えるための一時利用鍵および暗号化された一時利用鍵を生成する手段を具えたことを特徴とするホームメモリ。
【請求項５】　ホームメモリが生成した一時利用鍵および暗号化された一時利用鍵を取得する手段と、前記取得した暗号化された一時利用鍵を交換機に送出する手段と、前記取得した一時利用鍵により前記交換機との間で認証を行う手段とを具えたことを特徴とする移動機。
【請求項６】　移動機から送信された暗号化された一時利用鍵を受信する手段と、前記受信された一時利用鍵を復号化鍵を用いて復号する手段と、前記復号された一時利用鍵により前記移動機との間で認証を行う手段とを具えたことを特徴とする交換機。
【請求項７】　請求項４のホームメモリと、請求項５の移動機と、請求項６の交換機とを具えたことを特徴とする移動通信システム。
【請求項８】　請求項４において、さらに、あらかじめ定めた限定された地域範囲毎に一時利用鍵および暗号化された一時利用鍵を新たに生成する手段を有することを特徴とするホームメモリ。
【請求項９】　請求項５において、さらに、あらかじめ定めた限定された地域範囲毎に前記ホームメモリが新たに生成した一時利用鍵および暗号化された一時利用鍵を取得する手段を有することを特徴とする移動機。
【請求項１０】　請求項６の交換機と、請求項８のホームメモリと、請求項９の移動機とを具えたことを特徴とする移動通信システム。
【請求項１１】　請求項６において、前記復号手段は、前記復号化鍵を時間の経過に従って変更する手段を有することを特徴とする交換機。
【請求項１２】　請求項４のホームメモリと、請求項５の移動機と、請求項１１の交換機とを具えたことを特徴とする移動通信システム。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はホームメモリのアクセスを減らす認証方式を利用する移動通信における認証方法および移動通信システムにかかわる。
【０００２】
【従来の技術】図８にＲＣＲ　ＳＴＤ２７Ｃに記されている従来の移動通信における認証方法を示す。このシステムは移動機１０１、交換機１０２、ホームメモリ１０３からなる。移動機１０１とホームメモリ１０３は秘密鍵Ｓを共有する。交換機１０２は移動機１０１の正当性をチェックする必要がある場合、ホームメモリ１０３から秘密鍵Ｓを読み出し、乱数を生成し、移動機１０１へ乱数を送信する。移動機１０１は乱数を受信すると秘密鍵Ｓと乱数を使い認証演算し、結果を交換機１０２へ送信する。交換機１０２は乱数と秘密鍵Ｓを使用して認証演算し、移動機１０１から受信した認証演算結果と比較する。交換機１０２は比較結果が一致するとその移動機１０１は正当であるとみなし、一致しないとその移動機は正当でない移動機とみなす。
【０００３】不正移動機は交換機１０２から乱数を受信しても秘密鍵Ｓがないため、正しい認証演算ができず、正しい演算結果を返すことができない。その結果交換機１０２はその移動機が正当でないことがわかる。
【０００４】
【発明が解決しようとする課題】従来の方式では認証が必要になる度に交換機１０２はホームメモリ１０３へアクセスを行った。その結果、認証が頻繁に必要になるとホームメモリアクセスが増え、ホームメモリ１０３に大きな処理能力が必要となった。
【０００５】そこで本発明の目的は以上のような問題を解消した移動通信における認証方法および移動通信システムを提供することにある。
【０００６】
【課題を解決するための手段】図１は上記課題を解決するための手段を示す。基本的な考え方は、あらかじめ移動機に認証鍵を送っておき、認証が必要になると移動機から交換機に認証鍵を渡すことで、ホームメモリアクセスを減らす方法である。
【０００７】移動機１とホームメモリ３は秘密鍵Ａを共有する。また、交換機２とホームメモリ３は秘密鍵Ｂを共有する。
【０００８】ホームメモリ３は、移動機１に固有な一時利用鍵Ｃを生成する。そして一時利用鍵Ｃと移動機番号をまとめて秘密鍵Ｂで暗号化する。さらに一時利用鍵Ｃとこの秘密鍵Ｂで暗号化したデータとをまとめ、秘密鍵Ａで暗号化する。ホームメモリ３はこの秘密鍵Ａで暗号化されたデータを移動機１に送出する。移動機１は秘密鍵Ａで暗号化されたデータを受け取ると、このデータを秘密鍵Ａを用いて復号化し、一時利用鍵Ｃと秘密鍵Ｂで

暗号化されたデータを得て、これを記憶する。

【０００９】秘密鍵Ａと秘密鍵Ｂを共に知っているのはホームメモリ３だけであり、この秘密鍵Ａで暗号化されたデータはホームメモリ３にしか作れないため、暗号化データの作成に関してはセキュリティが保てる。

【００１０】また、他の移動機などは秘密鍵Ａを知らないので、暗号化データを盗聴しても、秘密鍵Ａで暗号化されたデータの解読はできない。

【００１１】次に認証が必要になると、移動機１は交換機２に秘密鍵Ｂで暗号化されたデータを送信する。交換機２は秘密鍵Ｂで暗号化されたデータを秘密鍵Ｂを用いて復号化し、移動機番号と一時利用鍵Ｃを得る。さらに、移動機番号を確認した後、一時利用鍵Ｃを用いて移動機１の認証を行う。

【００１２】秘密鍵Ｂを知っているのはホームメモリ３と交換機２のみであるため、移動機１がこの秘密鍵Ｂで暗号化されたデータを偽造することはできない。また、秘密鍵Ｂで暗号化されたデータには移動機番号が含まれるため、該当移動機以外がこのデータを利用することもできない。

【００１３】また、他人が盗聴しても秘密鍵Ｂを知らないため、復号化することはできない。

【００１４】上記手順により移動機１と交換機２は他人に知られることなく一時利用鍵Ｃを共有化することができ、この一時利用鍵Ｃにより交換機２は移動機１の認証ができる。

【００１５】暗号解読において、暗号文が多数手にはいるほど、また、平文と暗号文の組み合わせが多数手にはいるほど、暗号が破られ、秘密鍵の秘密性が保てなくなる可能性は高くなる。

【００１６】上記において秘密鍵Ｂは複数の交換機で共通の鍵を使用し、またすべての移動機に対して共通の鍵を使用する。その結果秘密鍵Ｂの使用頻度は多くなり、秘密鍵Ｂの秘密が保てない可能性も高くなる。この可能性を減らすため、秘密鍵Ｂの使用回数を減らす、以下の２つの方法がある。

【００１７】図２に第１の方法を示す。移動通信のエリアは着信の呼出エリアを限定するため複数の位置登録エリア（図２では地域１、地域２）に区切られており、移動機１は位置登録エリアを移動する度にホームメモリ３の位置登録エリアを登録する。

【００１８】この位置登録エリア毎に秘密鍵Ｂを変えることで、一つの秘密鍵Ｂの使用頻度と範囲は限定される。移動機１は位置登録エリアを移行する毎に位置登録と、さらに一時利用鍵Ｃの受け取りを行う。

【００１９】図３に第２の方法を示す。ホームメモリ３は秘密鍵Ｂを時間と共に変更し、交換機２に配送する。交換機２は発行時間別の秘密鍵Ｂのリストを持ち、発行時刻により、復号化に使用する秘密鍵Ｂを使い分ける。一時利用鍵Ｃには利用期限を設け、利用期限が来ると一時利用鍵Ｃと秘密鍵Ｂを破棄する。

【００２０】以上から、請求項１にかかる発明は、ホームメモリが生成した一時利用鍵と暗号化された一時利用鍵とを移動機が取得した後、前記移動機から前記暗号化された一時利用鍵を交換機に送信し、前記交換機が復号化鍵を用いて前記暗号化された一時利用鍵を復号した後、前記移動機と前記交換機との間で共有した前記一時利用鍵により認証を行うことを特徴とする。

【００２１】また、請求項２にかかる発明は、請求項１において、前記移動機は、あらかじめ定めた限定された地域範囲毎に前記ホームメモリが新たに生成した一時利用鍵および暗号化された一時利用鍵を取得することを特徴とする。

【００２２】さらに、請求項３にかかる発明は、請求項１において、前記交換機は、前記復号化鍵を時間の経過に従って変更することによって前記一時利用鍵の利用できる時間を制限することを特徴とする。

【００２３】さらに、請求項４にかかる発明は、移動機に与えるための一時利用鍵および暗号化された一時利用鍵を生成する手段を具えたことを特徴とする。

【００２４】さらに、請求項５にかかる発明は、ホームメモリが生成した一時利用鍵および暗号化された一時利用鍵を取得する手段と、前記取得した暗号化された一時利用鍵を交換機に送出する手段と、前記取得した一時利用鍵により前記交換機との間で認証を行う手段とを具えたことを特徴とする。

【００２５】さらに、請求項６にかかる発明は、移動機から送信された暗号化された一時利用鍵を受信する手段と、前記受信された一時利用鍵を復号化鍵を用いて復号する手段と、前記復号された一時利用鍵により前記移動機との間で認証を行う手段とを具えたことを特徴とする。

【００２６】さらに、請求項７にかかる発明は、請求項４のホームメモリと、請求項５の移動機と、請求項６の交換機とを具えたことを特徴とする。

【００２７】さらに、請求項８にかかる発明は、請求項４において、さらに、あらかじめ定めた限定された地域範囲毎に一時利用鍵および暗号化された一時利用鍵を新たに生成する手段を有することを特徴とする。

【００２８】さらに、請求項９にかかる発明は、請求項５において、さらに、あらかじめ定めた限定された地域範囲毎に前記ホームメモリが新たに生成した一時利用鍵および暗号化された一時利用鍵を取得する手段を有することを特徴とする。

【００２９】さらに、請求項１０にかかる発明は、請求項６の交換機と、請求項８のホームメモリと、請求項９の移動機とを具えたことを特徴とする。

【００３０】さらに、請求項１１にかかる発明は、請求項６において、前記復号手段は、前記復号化鍵を時間の経過に従って変更する手段を有することを特徴とする。

【００３１】さらに、請求項１２にかかる発明は、請求項４のホームメモリと、請求項５の移動機と、請求項１１の交換機とを具えたことを特徴とする。

【００３２】

【発明の実施の形態】図４に本発明の実施形態の一例を示す。この例は、移動機１と交換機２とホームメモリ３とからなる。

【００３３】移動機１は、秘密鍵Ａを記憶する秘密鍵Ａ記憶部４、一時利用鍵Ｃを記憶する一時利用鍵Ｃ記憶部５、暗号化データを記憶する暗号化データ記憶部６、復号化機能部７、入出力（送受信）部８および制御部９を有する。制御部９はこれらの各構成４～８を制御し、後述（図６，図７）の各制御手順に従う制御を行うものであって、そのためのＣＰＵ，ＲＯＭ，ＲＡＭ等から構成される。入出力部８は各記憶部４～６および制御部９と交換機２およびホームメモリ３との間のデータ（信号）の授受を行う。復号化機能部７は各記憶部４～６内のデータを参照して入力されたデータを必要に応じて復号する。

【００３４】交換機２は、時間別秘密鍵Ｂリスト記憶部１０、復号化機能部１１、入出力部１２および制御部１３を有する。制御部１３はこれらの各構成１０～１２を制御し、後述（図５～図７）の各制御手順に従う制御を行うものであって、そのためのＣＰＵおよびＲＯＭ，ＲＡＭ，ハードディスク等の記憶手段等から構成される。入出力部１２は、記憶部１０および制御部１３と移動機１およびホームメモリ３との間のデータ（信号）の授受を行う。時間別秘密鍵Ｂリスト記憶部１０は、発行時刻とこれに対応する秘密鍵Ｂのリストを記憶する。復号化機能部１１は記憶部１０内のデータを参照して入力されたデータを必要に応じて復号する。

【００３５】ホームメモリ３は、移動機毎の秘密鍵Ａを記憶する秘密鍵Ａ記憶部１４、地域別秘密鍵Ｂリスト記憶部１５、暗号化機能部１６、入出力部１７および制御部１８を有する。制御部１８はこれらの各構成１４～１７を制御し、後述（図５，図６）の各制御手順に従う制御を行うものであって、そのためのＣＰＵおよびＲＯＭ，ＲＡＭ，ハードディスク等の記憶手段等から構成される。入出力部１７は各記憶部１４，１５および制御部１８と移動機１および交換機２との間のデータ（信号）の授受を行う。地域別秘密鍵Ｂリスト記憶部１５は、地域とこれに対応する秘密鍵Ｂのリストを記憶する。暗号化機能部１６は、後述のように、各記憶部１４，１５内のデータ（秘密鍵Ａ，Ｂ）によって、一時利用鍵Ｃ、移動機番号等を暗号化する。

【００３６】図５にホームメモリ３が秘密鍵Ｂを生成し、交換機２に配送する手順を示す。ホームメモリ３は秘密鍵Ｂを生成すると、秘密鍵Ｂを記憶し、秘密鍵Ｂと使用開始時刻を含む秘密鍵Ｂ配送信号により交換機２に秘密鍵Ｂを配送する。秘密鍵Ｂ配送信号を受けた交換機２は、時間別秘密鍵Ｂリスト記憶部１０に使用開始時刻と秘密鍵Ｂを記憶する。また、一時利用鍵Ｃに使用期限がある場合、対応する一時利用鍵Ｃが期限切れとなり、使用することのない秘密鍵Ｂを削除しても良い。

【００３７】なお、ホームメモリ３において、秘密鍵Ｂを生成するタイミングは一定時間毎でもよいし、一時利用鍵Ｃを一定個数発行する毎でもよいし、あるいは不定期間隔でも良い。また、秘密鍵Ｂ配送信号が盗聴されると、秘密鍵Ｂの秘密性が保てなくなるため、十分セキュリティの高い方法で配送する必要がある。

【００３８】図６に移動機１が、位置登録エリアの移動や、一時利用鍵Ｃの期限切れで、ホームメモリ３が新たに一時利用鍵Ｃを発行する手順を示す。

【００３９】移動機１は移動機番号を含む位置登録要求を交換機２に送信する。

【００４０】位置登録要求を受信した交換機２は移動機番号からこの移動機１のホームメモリ３を探し、移動機番号を含む認証情報読出要求をそのホームメモリ３に送信する。

【００４１】認証情報読出要求信号を受信したホームメモリ３は、該当移動機１のデータを検索し、秘密鍵Ｓを含む認証情報読出応答を交換機２に送信する。

【００４２】認証情報読出応答を受信した交換機２は乱数を生成し、認証要求信号により乱数を移動機１に送信する。

【００４３】認証要求信号を要求した移動機１は乱数とあらかじめ持っている秘密鍵Ｓから認証演算を行い、認証演算結果を含む認証応答信号を交換機２に送信する。

【００４４】交換機２は乱数と秘密鍵Ｓから認証演算を行い、移動機１から受信した認証演算結果と比較する。比較結果が一致しないと、移動機１に位置登録拒否を送信する。比較結果が一致すると、ホームメモリ３に対して移動機番号を含む一時利用鍵発行要求を送信する。

【００４５】一時利用鍵発行要求を受信したホームメモリ３は当該交換機にかかる位置登録エリアを登録し、一時利用鍵Ｃを生成し、秘密鍵Ｂおよび秘密鍵Ａを使用して暗号化データ、すなわち、一時利用鍵Ｃおよび移動機番号を秘密鍵Ｂで暗号化し、これと、一時利用鍵Ｃおよび鍵発行時刻とを秘密鍵Ａで暗号化した暗号化データを作り、一時利用鍵発行応答で交換機２に送出する。

【００４６】一時利用鍵発行応答を受信した交換機２は、暗号化データを含む位置登録応答を移動機１に送出する。この位置登録応答を受信した移動機１はこれを秘密鍵Ａで復号する（この結果、一時利用鍵Ｃおよび鍵発行時刻が復号され、これらは記憶される）。

【００４７】なお、この例においては信号数の削除のため、位置登録と一時利用鍵Ｃの発行手順を同時に行っているが、分けて行ってもかまわない。また、秘密鍵Ｓを交換機２に送信して、交換機２が乱数の生成と認証演算を行っていたが、ホームメモリ３で乱数の生成と、認証

演算を行い、交換機には、認証情報読出応答で乱数と認証演算結果を送信してもよい。

【００４８】図７に一時利用鍵Ｃを利用するサービス手順を示す。

【００４９】移動機１は、移動機番号、鍵発行時刻、暗号化データを含むサービス要求を交換機２に送信する。この復号化データは、位置登録時に得た暗号化データを、秘密鍵Ａで解読することによって得られた秘密鍵Ｂで暗号化されている暗号化データであり、一時利用鍵Ｃと移動機番号のデータを含んでいる。

【００５０】サービス要求を受信した交換機２は、鍵発行時刻に対応する秘密鍵Ｂを、時間別秘密鍵Ｂリスト記憶部１０から選び、これによって暗号化データを復号化する。この復号化に失敗すると、交換機２は移動機１にサービス拒否を通知する。また、復号化したデータの中に含まれる移動機番号の値とサービス要求信号中の移動機番号が異なる場合も交換機２は移動機１にサービス拒否を通知する。

【００５１】交換機２は、正常に復号化でき、内容が正常であることを確認すると、次に移動機１が一時利用鍵を持っているかどうか確認するために、乱数を生成し、移動機１に乱数を含むローカル認証要求を送信する。

【００５２】ローカル認証要求信号を受信した移動機１は乱数と一時利用鍵Ｃから認証演算を行い、認証演算結果を含む認証応答信号を交換機２に送信する。

【００５３】交換機２は乱数と一時利用鍵Ｃから認証演算を行い、移動機から受信した認証演算結果と比較する。比較結果が一致しないと、移動機１にサービス拒否を送信する。比較結果が一致すると、交換機２はサービスを開始する。

【００５４】上記において、鍵発行時刻は時間別秘密鍵Ｂリスト記憶部１０のどの値を利用するかを決めるものであるため、現実の時刻でなく、秘密鍵Ｂを作りなおす度に増えるような数あるいは、時間別秘密鍵Ｂリスト記憶部１０の中のどの鍵を使用しているか示すようなインデックスでもよい。

【００５５】

【発明の効果】本発明によれば、ホームメモリにアクセスすることなく交換機が移動機の正当性を知ることができ、ホームメモリアクセスの回数を減少することができる。

【図面の簡単な説明】

【図１】本発明における課題を解決するための手段を示す図である。

【図２】秘密鍵Ｂの使用回数を減らすための一方法を説明する図である。

【図３】秘密鍵Ｂの使用回数を減らすための他の一方法を説明する図である。

【図４】本発明の実施形態の一例を示す図である。

【図５】本発明における制御手順の一例を示す図である。

【図６】本発明における制御手順の他の一例を示す図である。

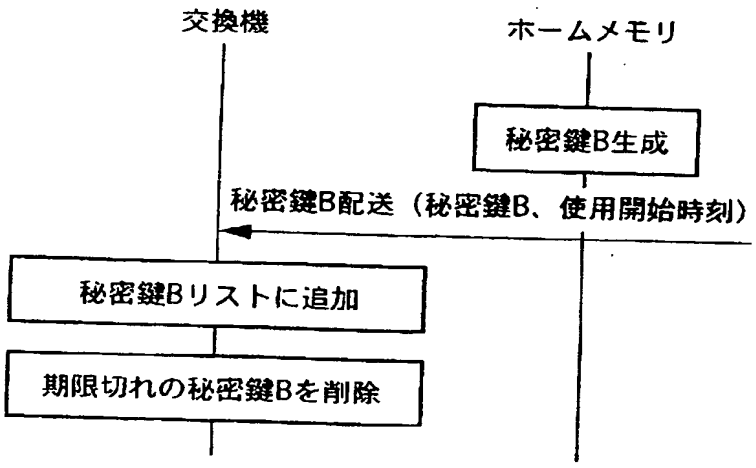
【図７】本発明における制御手順のさらに他の一例を示す図である。

【図８】従来例を示す図である。

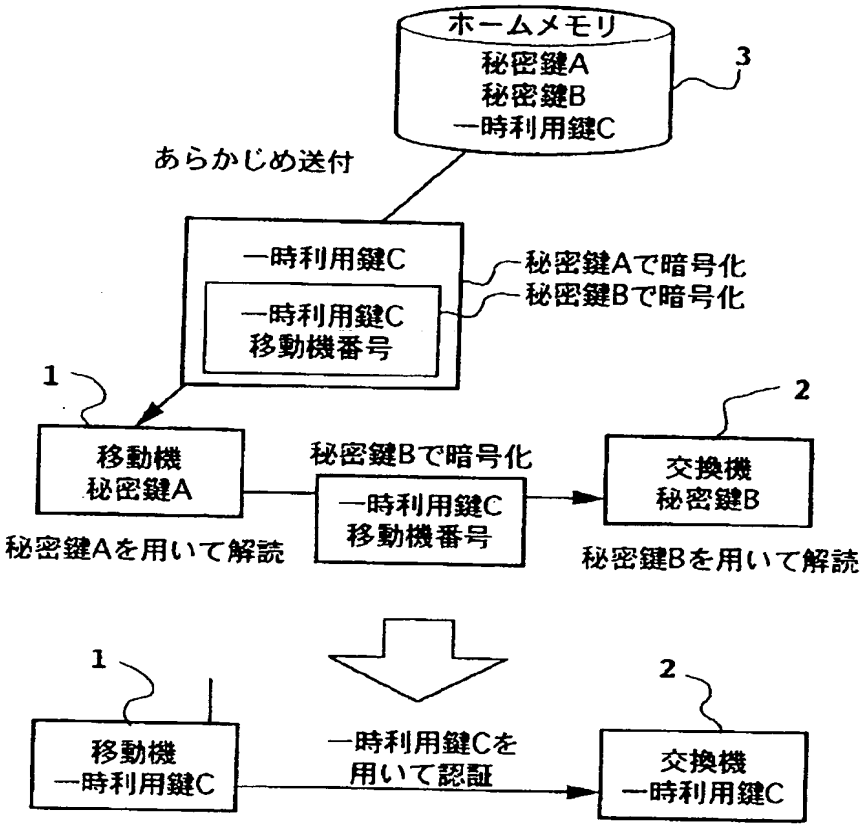
【符号の説明】

１　移動機
２　交換機
３　ホームメモリ

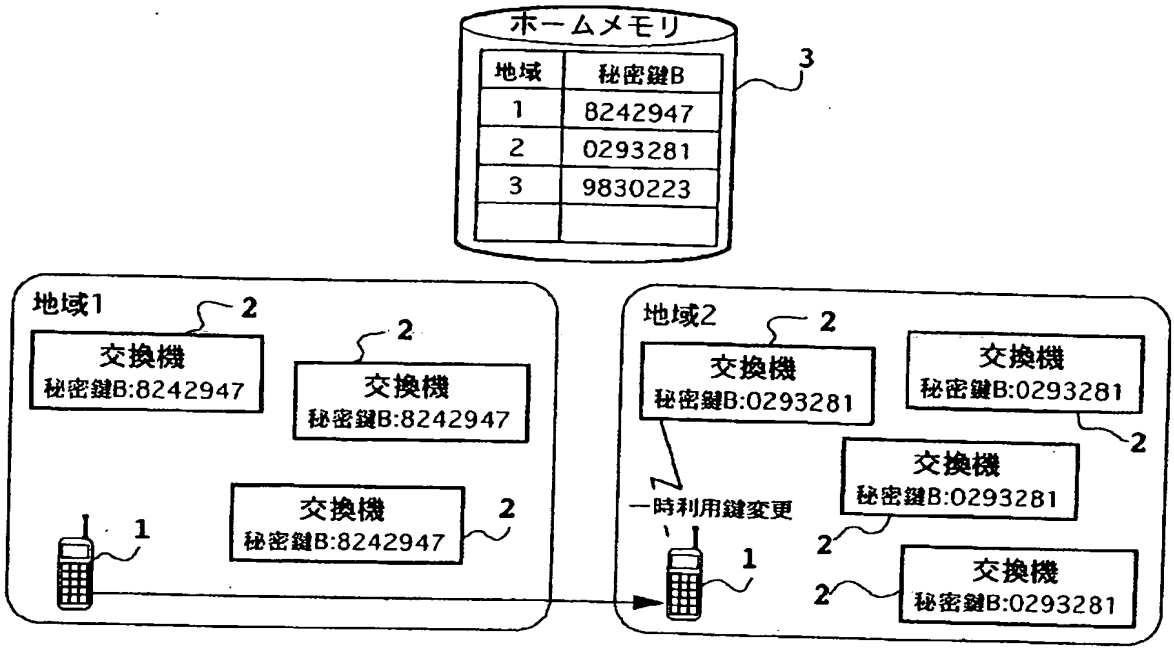
【図５】



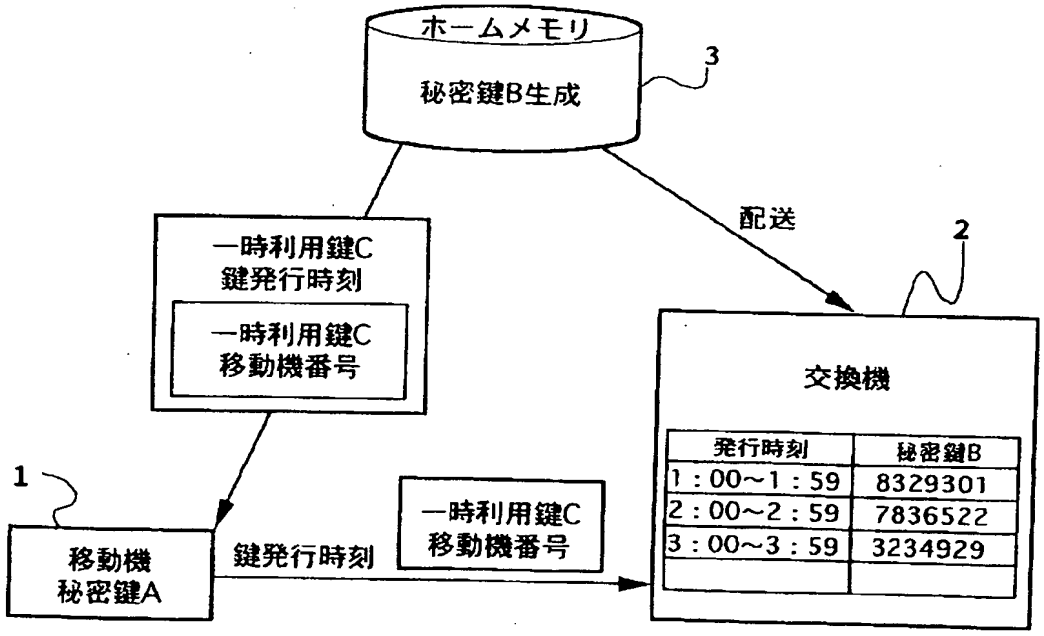
【図1】


ホームメモリ
秘密鍵A
秘密鍵B
一時利用鍵C
3
あらかじめ送付
一時利用鍵C
一時利用鍵C
移動機番号
秘密鍵Aで暗号化
秘密鍵Bで暗号化
1
2
移動機
秘密鍵A
秘密鍵Bで暗号化
一時利用鍵C
移動機番号
交換機
秘密鍵B
秘密鍵Aを用いて解読
秘密鍵Bを用いて解読
1
2
移動機
一時利用鍵C
一時利用鍵Cを
用いて認証
交換機
一時利用鍵C

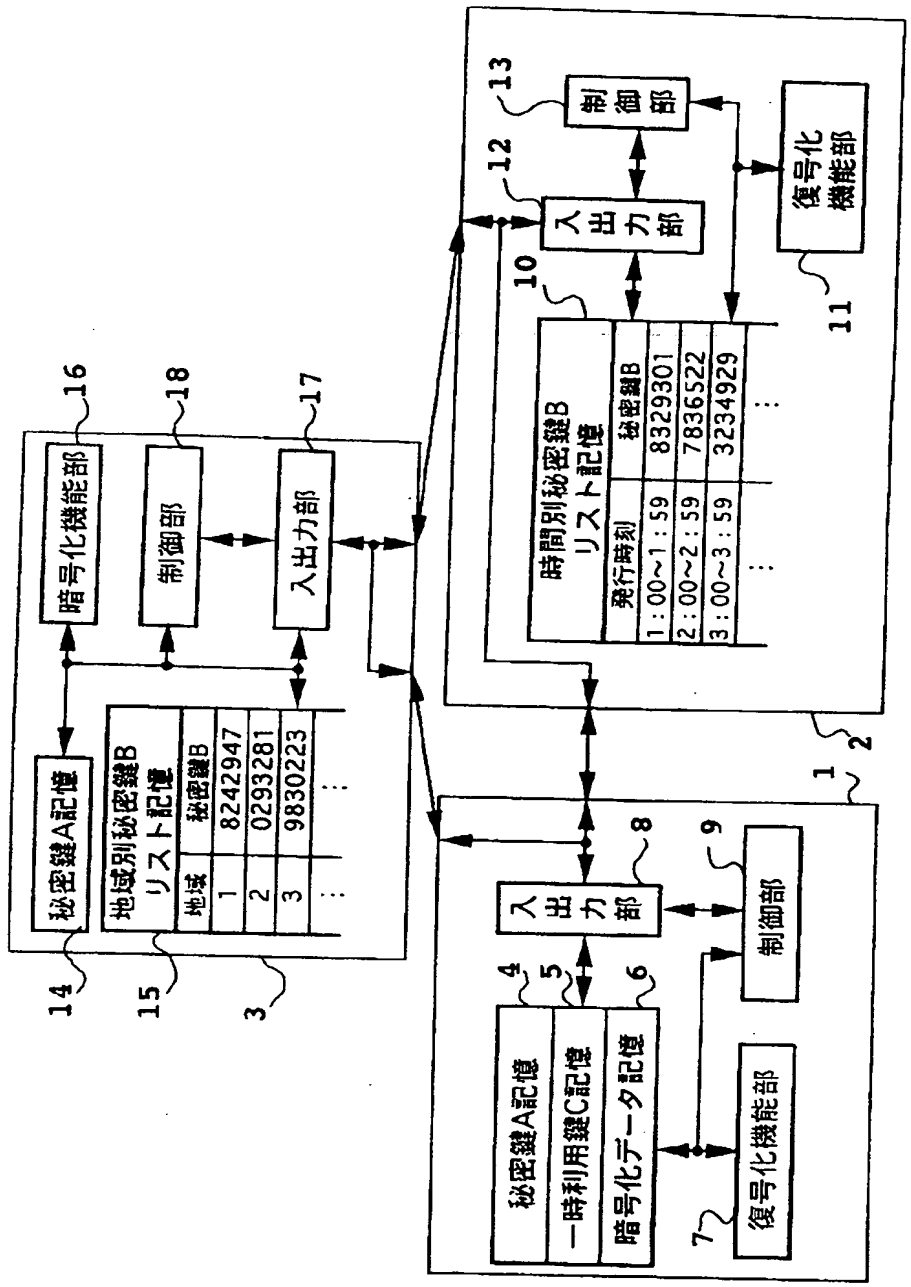
【図2】


ホームメモリ
地域
秘密鍵B
1
8242947
2
0293281
3
9830223
3
地域1
2
交換機
秘密鍵B:8242947
2
交換機
秘密鍵B:8242947
交換機
秘密鍵B:8242947
2
1
地域2
2
交換機
秘密鍵B:0293281
交換機
秘密鍵B:0293281
2
交換機
秘密鍵B:0293281
一時利用鍵変更
2
1
2
交換機
秘密鍵B:0293281

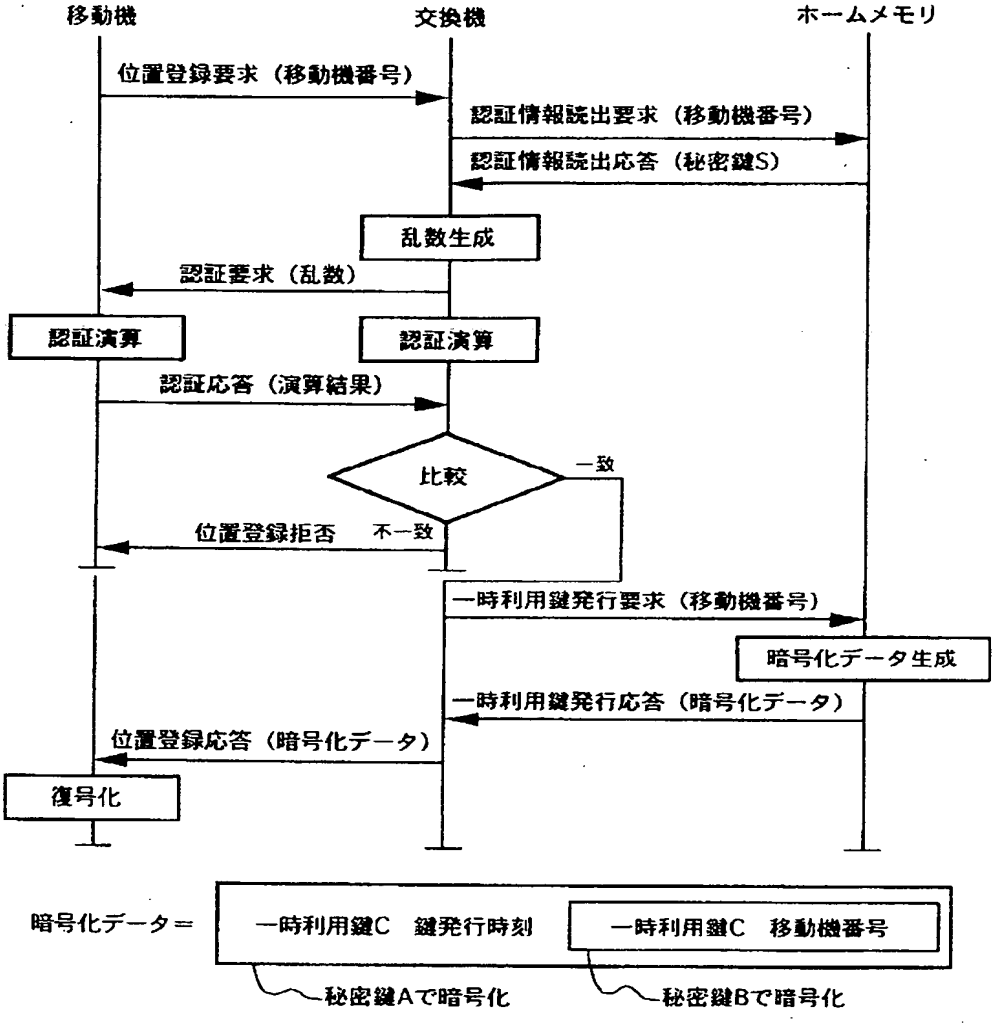
【図3】


ホームメモリ
秘密鍵B生成
3
配送
2
一時利用鍵C
鍵発行時刻
一時利用鍵C
移動機番号
交換機
発行時刻
秘密鍵B
1：00～1：59
8329301
2：00～2：59
7836522
3：00～3：59
3234929
1
移動機
秘密鍵A
鍵発行時刻
一時利用鍵C
移動機番号

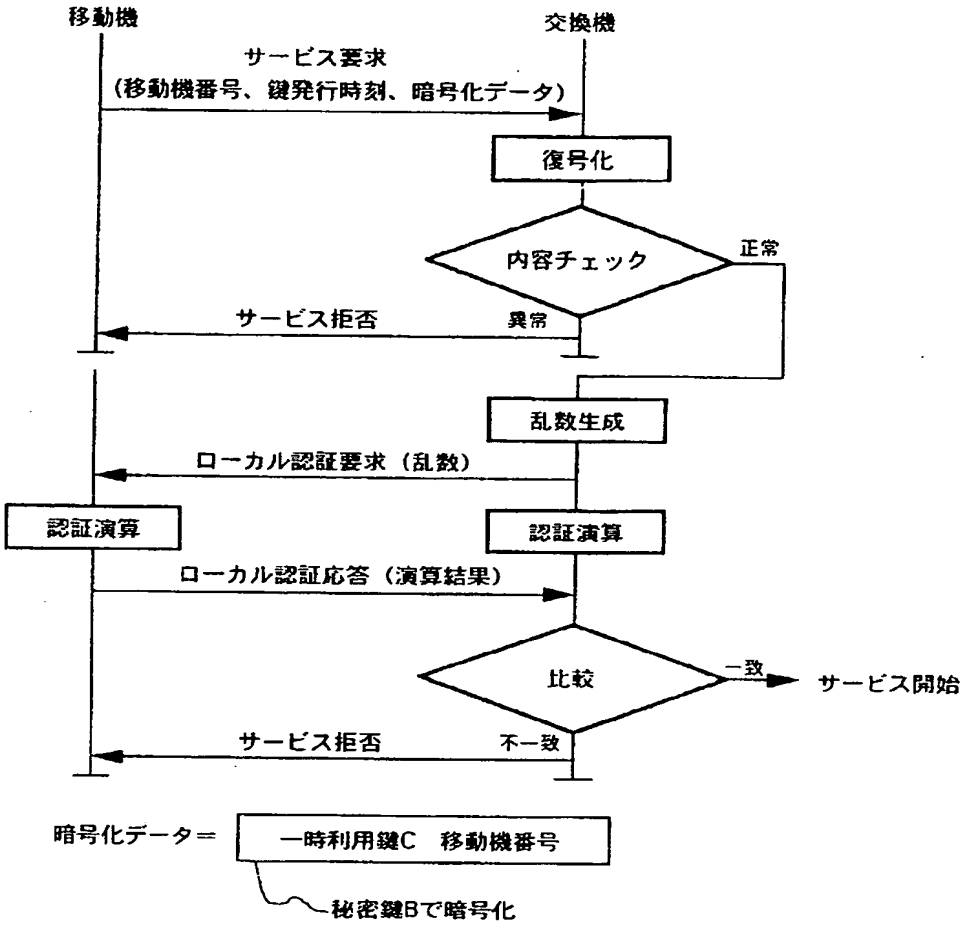
【図4】


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
秘密鍵A記憶
一時利用鍵C記憶
暗号化データ記憶
入出力部
制御部
復号化機能部
時間別秘密鍵B
リスト記憶
発行時刻
秘密鍵B
1:00～1:59
2:00～2:59
3:00～3:59
8329301
7836522
3234929
地域別秘密鍵B
リスト記憶
地域
1
2
3
8242947
0293281
9830223
暗号化機能部

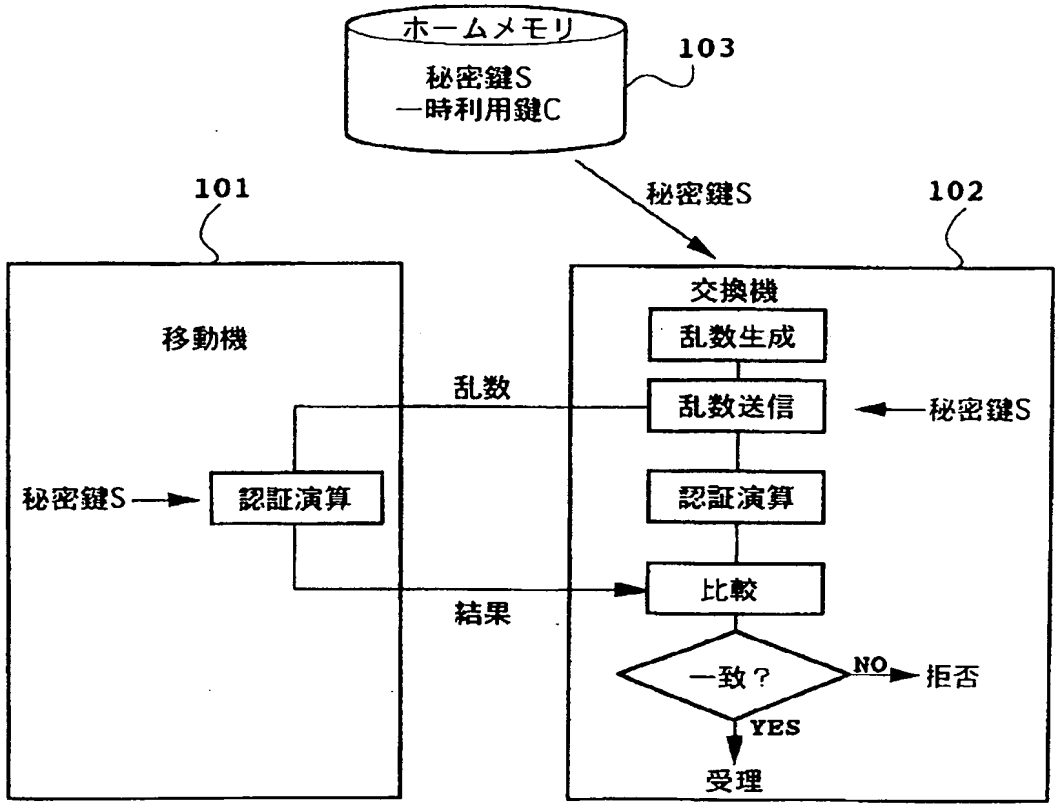
【図6】


移動機
交換機
ホームメモリ
位置登録要求（移動機番号）
認証情報読出要求（移動機番号）
認証情報読出応答（秘密鍵S）
乱数生成
認証要求（乱数）
認証演算
認証演算
認証応答（演算結果）
比較
一致
位置登録拒否
不一致
一時利用鍵発行要求（移動機番号）
暗号化データ生成
一時利用鍵発行応答（暗号化データ）
位置登録応答（暗号化データ）
復号化
暗号化データ＝
一時利用鍵C　鍵発行時刻
一時利用鍵C　移動機番号
秘密鍵Aで暗号化
秘密鍵Bで暗号化

【図7】


移動機
交換機
サービス要求
（移動機番号、鍵発行時刻、暗号化データ）
復号化
内容チェック
正常
サービス拒否
異常
乱数生成
ローカル認証要求（乱数）
認証演算
認証演算
ローカル認証応答（演算結果）
比較
一致
サービス開始
サービス拒否
不一致
暗号化データ＝
一時利用鍵C　移動機番号
秘密鍵Bで暗号化

【図8】


ホームメモリ
秘密鍵S
一時利用鍵C
103
101
秘密鍵S
102
移動機
交換機
乱数生成
乱数
乱数送信
秘密鍵S
秘密鍵S
認証演算
認証演算
比較
結果
一致？
NO
拒否
YES
受理

ABSTRACTS OF JP 09 – 051575

AUTHENTICATING METHOD FOR MOBILE COMMUNICATION AND MOBILE COMMUNICATION SYSTEM

Abstract:

PROBLEM TO BE SOLVED: To reduce home memory access by sending an authentication key to a mobile terminal in advance and passing the authentication key to an exchange from the mobile terminal when authentication is needed.

SOLUTION: A home memory 3 generates a temporary use key C which is characteristic of the mobile terminal 1. Then the temporary use key C and a mobile terminal number are both ciphered together with a secret key B. Further, the temporary use key C and the data ciphered with this secret key B are put together and the data ciphered with the secret key A are sent out to the mobile terminal 1. The mobile terminal 1 once receiving the ciphered data deciphers the data by using the secret key A to obtain the data ciphered with the temporary use key C and secret key B, and stored the data. When authentication is need, the mobile terminal 1 deciphers the data, ciphered with the secret key B, by using the secret key B to obtain the mobile terminal number and temporary use key C. Further, the mobile terminal number is confirmed and the mobile